IN THE CLAIMS:

The text of all pending claims are set forth below. Cancelled and withdrawn claims are indicated with claim number and status only. The claims as listed below show added text with underlining and deleted text with ~~strikethrough~~. The status of each claim is indicated with one of (original), (currently amended), (previously presented), (cancelled), (withdrawn), or (new).

Please CANCEL claims 1-26 and ADD claims 27-44 in accordance with the following:

1-26. (cancelled)

27. (new) A signing apparatus used in an authentication system which uses authentication data created by applying one-way functions to information divisible into a plurality of data divisions thereof, the apparatus comprising:

a dividing unit which divides the information into the plurality of data divisions;

an authenticator creating unit which creates a first authenticator specific to one of the data divisions by applying a respective first one-way function to the one of the data divisions, and creates a second authenticator specific to an other one of the data divisions by applying a respective second one-way function using a second key to the other one of the data divisions, where the first and second keys are different; and

an appending unit which appends the first and second authenticators to the information for sending with the information to a certifying apparatus in the authentication system.

28. (new) The signing apparatus according to claim 27, wherein

the dividing unit divides the information into the plurality of data divisions each having a pre-specified length, and

the authenticator creating unit creates the first authenticator by applying the first one-way function to one of the data divisions to be applied and a last result of the first one-way function, and creates the second authenticator by applying the second one-way function to one of the data divisions to be applied and a last result of the second one-way function.

29. (new) The signing apparatus according to claim 27, wherein the appending unit appends authenticators obtained by truncating the first and second authenticators to the information.

30. (new) The signing apparatus according to claim 27, wherein the first and second one-way functions discretely and independently create the first and second authenticators in parallel.

31. (new) The signing apparatus according to claim 27, wherein intermediate data created by the first one-way function during its one-way operations is used by the second one-way function as an initial value to create the second authenticator.

32. (new) A certifying apparatus used in an authentication system which uses authentication data created by applying one-way functions to information divisible into a plurality of data divisions, the apparatus comprising:

a separating unit which separates out the information and a plurality of authenticators from authenticator-appended information which is received from a signing apparatus in the authentication system;

a dividing unit which divides the information separated out by the separating unit into the plurality of data divisions;

an authenticator creating unit which creates a first authenticator specific to one of the data divisions by applying a respective first one-way function using a first key to the one of the data divisions, and creates a second authenticator specific to an other one of the data divisions by applying a respective second one-way function using a second key to the other one of the data divisions, where the first and second keys are different; and

a certifying unit which authenticates the information by comparing the first authenticator with a third authenticator corresponding to the first authenticator of the authenticators separated out by the separating unit, and by comparing the second authenticator with a fourth authenticator corresponding to the second authenticator of the authenticators separated out by the separating unit.

33. (new) The certifying apparatus according to claim 32, wherein

the dividing unit divides the information separated out by the separating unit into the plurality of data divisions each having a pre-specified length,

the authenticator creating unit creates the first authenticator by applying the first one-way function to one of the data divisions to be applied and a last result of the first one-way function, and creates the second authenticator by applying the second one-way function to one of the data divisions to be applied and a last result of the second one-way function.

34. (new) The certifying apparatus according to claim 32, wherein the separating unit obtains truncated authenticators from the data received from the signing apparatus, and the certifying unit compares an authenticator obtained by truncating the first authenticator with the truncated third authenticator separated out by the separating unit, and compares an authenticator obtained by truncating the second authenticator with the truncated fourth authenticator separated out by the separating unit.

35. (new) The certifying apparatus according to claim 32, wherein the first and second one-way functions discretely and independently create the authenticators in parallel.

36. (new) The certifying apparatus according to claim 32, wherein intermediate data created by the first one-way function during its one-way operations is used by the second one-way function as an initial value to create the second authenticator.

37. (new) A signing method used in an authentication system which uses authentication data created by applying one-way functions to information divisible into a plurality of data divisions, the method comprising:

dividing the information into the plurality of data divisions;

creating a first authenticator specific to one of the data divisions by applying a respective first one-way function using a first key to the one of the data divisions, and creates a second authenticator specific to an other one of the data divisions by applying a respective second one-way function using a second key to the other one of the data divisions, where the first and second keys are different; and

appending the first and second authenticators to the information for sending with the information to a certifying apparatus in the authentication system.

38. (new) A certifying method used in an authentication system which uses authentication data created by applying one-way functions to information divisible into a plurality of data divisions, the method comprising:

separating out the information and a plurality of authenticators from authenticator-appended information which is received from a signing apparatus in the authentication system;

dividing the separated out information into the plurality of data divisions;

creating a first authenticator specific to one of the data divisions by applying a respective first one-way function using a first key to the one of the data divisions;

creating a second authenticator specific to an other one of the data divisions by applying a respective second one-way function using a second key to the other one of the data divisions, where the first and second keys are different;

authenticating the information by comparing the first authenticator with a third authenticator corresponding to the first authenticator of the separated-out authenticators, and by comparing the second authenticator with a fourth authenticator corresponding to the second authenticator of the separated-out authenticators.

39. (new) A computer program product for signing in an authentication system which uses authentication data created by applying one-way functions to information divisible into a plurality of data divisions, the computer program product including computer executable instructions stored on a computer readable medium, wherein the instructions, when executed by a computer, cause a computer to perform a process, the process comprising;

dividing the information into the plurality of data divisions;

creating a first authenticator specific to one of the data divisions by applying a respective first one-way function using a first key to the one of the data divisions, and creating a second authenticator specific to an other one of the data divisions by applying a respective second one-way function using a second key to the other one of the data divisions, where the first and second keys are different; and

appending the first and second authenticators to the information for sending with the information to a certifying apparatus in the authentication system.

40. (new) A computer program product for certifying in an authentication system which uses authentication data created by applying one-way functions to information divisible into a plurality of data divisions, the computer program product including computer executable instructions stored on a computer readable medium, wherein the instructions, when executed by a computer, cause a computer to perform a process, the process comprising:

separating out the information and a plurality of authenticators from authenticator-appended information received from a signing apparatus in the authentication system;

dividing the separated out information into the plurality of data divisions;

creating a first authenticator specific to one of the data divisions by applying a respective first one-way function using a first key to the one of the data divisions;

creating a second authenticator specific to an other one of the data divisions by applying a respective second one-way function using a second key to the other one of the data divisions, where the first and second keys are different;

authenticating the information by comparing the first authenticator with a third authenticator corresponding to the first authenticator of the separated-out authenticators, and by comparing the second authenticator with a fourth authenticator corresponding to the second authenticator of the separated-out authenticators.

41. (new) An authentication system uses authentication data created by applying one-way functions to information divisible into a plurality of data divisions, the system comprising:

a signing apparatus which includes

a first dividing unit which divides the information into the plurality of data divisions;

an authenticator creating unit which creates a first authenticator specific to one of the data divisions by applying a respective first one-way function using a first key to the one of the data divisions, and which creates a second authenticator specific to an other one of the data divisions by applying a second one-way function using a second key to the other one of the data divisions, where the first and second keys are different; and

an appending unit appends the first and second authenticators to the information for sending with the information to a certifying apparatus in the authentication system; and

a certifying apparatus which includes

a separating unit which separates out the information and a plurality of authenticators from the authenticator-appended information which is received from the signing apparatus in the authentication system;

a second dividing unit which divides the information separated out by the separating unit into the plurality of data divisions;

an authenticator creating unit which creates a first authenticator by applying a first one-way function using a first key to a respective one of the data divisions, and creates a second authenticator specific to another one of the data divisions by applying a second one-way function using a second key to the other one of the data divisions, where the first and second keys are different; and

a certifying unit which authenticates the information by comparing the first authenticator with a third authenticator corresponding to the first authenticator of the authenticators separated by the separating unit, and by comparing the second authenticator with a fourth authenticator corresponding to the second authenticator of the authenticators separated by the separating unit.

42. (new) An authentication method used in an authentication system which uses authentication data created by applying one-way functions to information divisible into a plurality of data divisions, the method comprising:

dividing the information into the plurality of data divisions;

creating a first authenticator specific to one of the data divisions by applying a respective first one-way function using a first key to the one of the data divisions, and creating a second authenticator specific to another one of the data divisions by applying a respective second one-way function using a second key to the other one of the data divisions, where the first and second keys are different;

appending the first and second authenticators to the information for sending with the information to a certifying apparatus in the authentication system;

sending the authenticator-appended information;

receiving and separating out the information and a plurality of authenticators from the sent authenticator-appended information;

dividing the separated-out information into the plurality of data divisions;

creating a first authenticator specific to one of the data divisions by applying a first one-way function using a first key to the one of the data divisions;

creating a second authenticator specific to another one of the data divisions by applying a second one-way function using a second key to the other one of the data divisions, where the first and second keys are different;

authenticating the information by comparing the first authenticator with a third authenticator, corresponding to the first authenticator of the separated-out authenticators, and by comparing the second authenticator with a fourth authenticator corresponding to the second authenticator of the separated-out authenticators.

43. (new) A computer program product for authentication in an authentication system which uses authentication data created by applying one-way functions to information divisible into a plurality of data divisions, the computer programs product including computer executable instructions stored on a computer readable medium, wherein the instructions, when executed by a computer, cause a computer to perform a process, the process comprising:

dividing the information into the plurality of data divisions;

creating a first authenticator specific to one of the data divisions by applying a first one-way function using a first key to the one of the data divisions, and creating a second authenticator specific to an other one of the data divisions by applying a respective second one-way function using a second key to the other one of the data divisions, where the first and second keys are different;

appending the first and second authenticators to the information for sending with the information to a certifying apparatus in the authentication system;

sending the authenticator-appended information;

receiving and separating out the information and a plurality of authenticators from the sent authenticator-appended information;

dividing the separated-out information into the plurality of data divisions;

creating a first authenticator specific to one of the data divisions by applying a respective first one-way function using a first key to the one of the data divisions;

creating a second authenticator specific to an other one of the data divisions by applying a respective second one-way function to the other one of the data divisions, where the first and second keys are different;

authenticating the information by comparing the first authenticator with a third authenticator corresponding to the first authenticator, of the separated-out authenticators, and by comparing the second authenticator with a fourth authenticator corresponding to the second authenticator of the separated-out authenticators.

44. (new) A method for an authentication system using plural one-way functions, the method comprising:

receiving text data to be signed;

dividing the text data into different data divisions;

for each data division, creating an authenticator specific to the data division by applying to the data division a different respective one of the one-way functions using a different key, whereby each data division's authenticator is produced by a different one-way function using a different key; and

signing the text data by appending the authenticators.